DOD Privacy Impact Assessment (PIA)

1. Name of MACOM / DA Staff Proponent (APMS Sub Organization Name)

U. S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System.

Mobilization Tracking System (CIVTRACKS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

2801

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 3013, Secretary of the Army;
DoDI 1400.32 DoD Civilian Workforce Contingency and Emergency Planning Guidelines and Procedures;
Army Regulation 690-200, General Personnel Provisions;
Executive Order 9397

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup)

The Civilian Mobilization Tracking System (CIVTRACKS) is a web-based application that provides the capability to track Army civilian employees and contractors, as well as Red Cross and AAFES employees deployed to a theater of operations, in any part of the world, in support of a contingency operation, or involved in a mobilization exercise. It is designed to provide a quick and efficient way to track movements of individuals during mobilization situations. CIVTRACKS is in the operation and maintenance phase. The system contains information pertaining to deployed Army civilian personnel, Army contractors, Red Cross employees, and AAFES employees.

The system interfaces with the Headquarters Army Civilian Personnel System (HQ ACPERS) through a secure encrypted network connection. Users can access an online application. Web servers, application servers and database servers are located in Alexandria, Virginia.

Full database backups are run daily. System event logs are checked daily by the administrator / information assurance security officer (IASO). Tapes are stored in a commercial facility in Atlanta, Georgia.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

Information in identifiable form that will be collected includes: individual's name, social security number (SSN), type of employee, home station, operation they are supporting, home address, email address, organization, pay plan, series grade, command code, unit identification, personnel office identifier, location traveled to and from, location arrival and location departure dates, point of contact information (including name, address and telephone number), DNA flags and expected return dates. Information in identifiable form is extracted from HQ ACPERS (the Army civilian workforce database repository) via a secure network system. Select information in identifiable form is collected directly from the individual via the CIVTRACKS web site.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Information is extracted from HQ ACPERS (the Army civilian workforce database repository) via a secure network connection. Select information is also collected directly from the individual via the CIVTRACKS web site.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

This system ensures proper tracking and accountability of Army civilian personnel deployed worldwide in support of contingency operations or mobilization exercises. Department of Defense requires that the Army must establish civilian work force

accountability procedures (i.e. names, numbers, locations, status, etc.) for civilian employees in theaters of operation. CIVTRACKS was developed to help carry out this mandate. Information in identifiable form is collected and used by this system in direct support of this mission.

13. Describe how the information in identifiable form will be used (e.g. to verify exiting data, etc.).

Information collected from the individual is matched and combined with information extracted from HQ ACPERS. This information will be used to track and account for civilian employees deployed to a theater of operations.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The system does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.) .

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Information is provided to the Commanders of civilian personnel who are deployed. Internal DoD agencies that would obtain access to Personally Identifiable information (PII) in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Manpower Data Center, Defense Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable for about themselves or to contest to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Personal data is voluntarily given by the applicant and collected via electronic form on the CIVTRACKS website. A Privacy Act advisory statement is displayed upon log-in to

the system. Information in identifiable form is also extracted from HQ ACPERS (the Army civilian workforce database repository) via a secure network system.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

A Privacy Act statement in written form describing the use, dissemination and collection of information in identifiable form is located on the web site on the page where the data is collected.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Users of this system include deployed individuals, management users, system administrators, developers and database administrators. The CIVTRACKS application does not allow deployed individuals to retrieve data from the database. All personnel accessing government computer information are required to undergo and receive at the minimum ADP/IT III background investigation. These users (both government and contractor) may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Management users as well system and database adminstrators must enter appropriate user identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is routine monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program" November 11, 2004. If so, and a System of Records Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when the publication of the notice will occur.

The system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risk regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate and privacy risks in providing individuals and opportunity to object/contest or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Information is protected by user passwords, Common Access Card (CAC) access, firewalls, antivirus software and data-at-rest protection on portable laptops thus the level risk with these adopted security measures is minimal.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.